Partial monoids: associativity and confluence

Laurent Poinsot, Gérard Henry Edmond Duchamp, Christophe Tollu

Partial monoids: associativity and confluence

Laurent Poinsot[1], Gérard H.E. Duchamp[1] and Christophe Tollu[1]

Université Paris-Nord, Institut Galilée,
Laboratoire d'Informatique de Paris-Nord, UMR CNRS 7030,
F-93430 Villetaneuse, France

Abstract. A partial monoid P is a set with a partial multiplication $\times$ (and total identity 1_P) which satisfies some associativity axiom. The partial monoid P may be embedded in the free monoid P^* and the product $\times$ is simulated by a string rewriting system on P^* that consists in evaluating the concatenation of two letters as a product in P, when it is defined, and a letter 1_P as the empty word ϵ. In this paper we study the profound relations between confluence for such a system and associativity of the multiplication. Moreover we develop a reduction strategy to ensure confluence and which allows us to define a multiplication on normal forms associative up to a given congruence of P^*. Finally we show that this operation is associative if, and only if, the rewriting system under consideration is confluent.
Key-words: Partial monoid, string rewriting system, normal form, associativity and confluence

1 Introduction

A partial monoid is a set equipped with a partially-defined multiplication, say $\times$, which is associative in the sense that $(x \times y) \times z = x \times (y \times z)$ means that the left-hand side is defined if, and only if, the right-hand side is defined, and in this situation they are equal. A partial monoid is also assumed to have an identity element. Our original interest on such structures is due to the fact that they provide an algebraic framework for an abstract notion of connected components and the treatment of the exponential formula [10].

However another interesting feature of partial monoids motivates our work: their interpretation as a model of computation with errors. Programs can be interpreted as partial functions and their composition, when defined, simulate a sequential process. Abstracting this situation by considering programs as elements of a partial monoid, the notion of error occurs naturally: an error is nothing but the evaluation of a not defined product. In order to locate the fault, we can set undefined products to be equal to some new symbol (an error flag), for instance 0, *i.e.*, $x \times y = 0$ when $x \times y$ is undefined. Now, if we interpret an n-fold product $x_1 \times x_2 \times \cdots \times x_n$ as some sequential program, then if the evaluation of one of the factors is an error, the program itself is erroneous, in other terms, $0 \times x = 0 = x \times 0$ for every x. This situation is not fully satisfactory for the reason that the factor whose evaluation causes the error is lost

by this crunch to zero. To fix this weakness, let us consider that the machine, which performs the execution $x_1 \times x_2 \times \cdots \times x_n$, evaluates a factor $x_i \times x_{i+1}$ only when it is defined. In other terms, the machine only deals with error-free factors. The result of such an execution is a " word " $u_1 \times \cdots \times u_k$ which may be seen as an exception handling: each factor u_i marks faultless computations, while a product $u_j \times u_{j+1}$ labels an error. Obviously a word reduced to a single element represents the result of a program with no error at all.

Mathematically speaking, the previous situation is perfectly described first by embedding the partial monoid P into the free monoid P^* of words over the alphabet P, and second, by mimicking the execution of a program $w \in P^*$ as applications of the rewriting rules: if $w = uxyv$ and $x \times y$ is defined in P, then $w \Rightarrow u(x \times y)v$, and if $w = u1_P v$ (1_P is the identity of P), then $w \Rightarrow uv$. Actually an execution as described above is represented by reductions of the word as far as it is possible. In other words, an execution computes – when it exists – the normal form of the program w. This string rewriting system – called a *semi-Thue system* – is easily seen to be terminating, *i.e.* without infinite executions, property which guarantees existence, but not uniqueness, of normal forms. Seen as the result of an execution, a normal form should be unique. This is possible when the semi-Thue system is *confluent*.

The main objective of this work is to highlight the profound links between associativity and confluence for such rewriting systems, that is, to give characterizations of confluence in terms of associativity, and *vice versa*. In this paper, we exhibit the exact property the partial monoids must satisfy to ensure confluence of the system. Since this particular property does not hold in every partial monoid, we develop a strategy of reduction, called the *left standard reduction*, which provides a unique normal form which is also a normal form for the initial system. Finally, using the left standard reduction, we equip the set of all normal forms with a total binary operation which is shown to be associative up to some monoidal congruence. In order to prove this result, we use another rewriting system on nonassociative words – which allows us to move pairs of brackets to perform associativity – in a way similar to the treatment of the coherence theorem for monoidal category [23]. Finally we show that the operation on normal forms is associative if, and only if, the semi-Thue system under consideration is confluent.

Note 1. Most of the proofs of lemmas will be omitted, since they are free of technical difficulties.

2 Partial monoids

A *partial monoid* (see [10,25,30]) – also sometimes called *premonoid* [3,4] – is a nonvoid set P together with a partially-defined function $\times : P \times P \to P$, with domain of definition $\mathsf{dom}(\times) \subseteq P \times P$, and a distinguished element, $1_P \in P$, called the *identity*, such that

1. for every $x \in P$, $(x, 1_P)$ and $(1_P, x)$ belong to $\mathsf{dom}(\times)$, and, $x \times 1_P = x = 1_P \times x$;

2. for every $x, y, z \in P$, $(x, y) \in \mathsf{dom}(\times)$, $(x \times y, z) \in \mathsf{dom}(\times)$ if, and only if, $(y, z) \in \mathsf{dom}(\times)$, $(x, y \times z) \in \mathsf{dom}(\times)$, and, in both cases, $(x \times y) \times z = x \times (y \times z)$.

Let us consider the set $P^0 = P \cup \{0\}$ obtained from P by the adjunction of a new element 0. The operation $\times$ is extended to the whole Cartesian product $P^0 \times P^0$ as an operation $\times^0$ by setting $x \times^0 y = x \times y$ for every $(x, y) \in \mathsf{dom}(\times)$ and $x \times^0 y = 0$ for remaining pairs of elements of P^0. This new structure is a monoid (see [22]). From this we deduce that given $(x_1, \cdots, x_n) \in P^n$, if the n-fold product is defined for a particular choice of brackets, then it is defined for all bracketings, and the values are equal.

Example 1. 1. Let X be any set, and 2^X be the set of its subsets. We endow 2^X with the *disjoint union* defined only for non-intersecting subsets. Then, 2^X is a partial monoid with $\emptyset$ as identity. Such monoids are useful to define a general setting for the exponential formula of combinatorics [10].
2. Let us consider the set

$$P = \{\epsilon, a, b, c, ab, ac, ba, bc, ca, cb, abc, acb, bac, bca, cab, cba\} \tag{1}$$

with the product $\times$ being concatenation of two words without common letters. Then P is a partial monoid with the empty word ϵ as its identity.

3 Basics on rewriting rules and normal forms

3.1 Abstract rewriting systems

An *abstract rewriting system* (see [1,29] for more details) is a pair $(S, \Rightarrow)$ where S is a set and $\Rightarrow$ is a binary relation on S, called *one-step rewriting* or *reduction relation*. If $(a, b) \in \Rightarrow$, then we write $a \Rightarrow b$ (" *a is reduced by $\Rightarrow$ to b* " and a is said to be *reducible*). The reflexive-transitive closure $\Rightarrow^*$ of $\Rightarrow$ is called the *many-step rewriting relation* generated by $\Rightarrow$, while its symmetric-reflexive-transitive closure $\Leftrightarrow^*$, *i.e.*, the equivalence relation generated by $\Rightarrow$, is called the *convertibility relation* (generated by $\Rightarrow$). An abstract rewriting system is said to be

1. *terminating* if, and only if, $\Rightarrow$ is Noetherian;
2. *confluent* if, and only if, for every $a, b, c \in S$ such that $a \Rightarrow^* b$ and $a \Rightarrow^* c$, there is d such that $b \Rightarrow^* d$ and $c \Rightarrow^* d$;
3. *locally confluent* if, and only if, for every $a, b, c \in S$ such that $a \Rightarrow b$ and $a \Rightarrow c$, there is d such that $b \Rightarrow^* d$ and $c \Rightarrow^* d$.

If $a \in S$ is minimal with respect to $\Rightarrow$, *i.e.*, there is no b such that $a \Rightarrow b$, then a is called a $\Rightarrow$-*normal form* or, simply, a *normal form*, or a is said *irreducible* (with respect to $\Rightarrow$). The set of all irreducible elements of S is denoted $\mathsf{Irr}(S, \Rightarrow)$ or simply $\mathsf{Irr}(S)$ or $\mathsf{Irr}(\Rightarrow)$. If $a \in S$ and $b \in \mathsf{Irr}(S)$ such that $a \Rightarrow^* b$, then b is called a *normal form of* a. In a terminating abstract rewriting system, every element has at least one normal form, and in a confluent abstract rewriting system the normal form of any element, if it exists, is unique [15].

Lemma 1 ((Newman's lemma [15,24,29])). *A terminating abstract rewriting system is confluent if, and only if, it is locally confluent.*

Therefore in a terminating and confluent abstract rewriting system, every element has a unique normal form.

3.2 Semi-Thue system

See [7,17] for more details on string rewriting, and [5] for rewriting systems over algebraic structures. Let X be any set. A *semi-Thue system* R on X is a binary relation on X^*. An element of R is called a(n) *(elementary) rule*. The *(single-step) reduction relation* on X^* induced by the rules of R is defined as follows: $uav \Rightarrow_R ubv$ whenever $u, v \in P^*$ and $(a, b) \in R$. Thus $(X^*, \Rightarrow_R)$ is an abstract rewriting system on X^*. We say that R is locally confluent (resp. confluent, terminating) if the corresponding property holds for the abstract rewriting system $(X^*, \Rightarrow_R)$. We use $\mathsf{Irr}(X)$ or $\mathsf{Irr}(R)$ to denote $\mathsf{Irr}(X^*, \Rightarrow_R)$. The reflexive-transitive closure $\Rightarrow_R^*$ of $\Rightarrow_R$ is called the *reduction rule generated by* R. It can be seen as the smallest quasi-order relation containing R which is compatible with concatenation ([19]). The convertibility relation $\Leftrightarrow_R^*$ (generated by $\Rightarrow_R$) is nothing else than the congruence generated by R, and called the *Thue congruence* induced (or generated) by R. A pair $(u, v) \in X^* \times X^*$ is called a *critical pair (of R)* if, and only if, u, v have either the form $u = u_1 r_1$, $v = r_2 v_2$ for some $u_1, v_1 \in X^*$, $(\ell_1, r_1), (\ell_2, r_2) \in R$, $u_1 \ell_1 = \ell_2 v_2$ and $|u_1| < |\ell_2|$ ($|w|$ is the length of a word w), or $u = r_1$, $v = v_1 r_2 v_2$ for some $v_1, v_2 \in X^*$, (ℓ_1, r_1), (ℓ_2, r_2) and $\ell_1 = v_1 \ell_2 v_2$. A critical pair of the first kind is called an *overlap ambiguity*, while a critical pair of the second kind is an *inclusion ambiguity*. A critical pair (u, v) is *convergent* if there is $w \in X^*$ such that $u \Rightarrow_R^* w$ and $v \Rightarrow_R^* w$. A critical pair (u, v) such that $u = v$ is called *trivial*. If a Thue system is known to be terminating, then local confluence – and hence confluence – holds if, and only if, each critical pair is convergent [15] (actually this is a more general result that holds for term rewriting systems).

4 Semi-Thue system associated with a partial monoid

4.1 First definitions

Given a partial monoid P. Let $i_P : P \hookrightarrow P^*$ be the natural injection. Any element of P^* may be written in a unique way as a word $i_P(x_1) \cdots i_P(x_n)$ for some $n \in \mathbb{N}$ and $x_i \in P$ ($n = 0$ leads to the empty word ϵ). Moreover we sometimes use the notation $u = u_1 \cdots u_n$ with the meaning that $u_i = i_P(x_i)$. We define the following semi-Thue system $R_P = \{(i_P(x) i_P(y), i_P(x \times y)) : (x, y) \in \mathsf{dom}(\times)\} \cup \{(i_P(1_P), \epsilon)\}$, call it *the semi-Thue system associated with* P, which is easily seen to be terminating. A similar idea has been used in [2,3,4,9,28] (see also [26]). In what follows, when it is possible R_P is denoted by R. The set of irreducible elements $\mathsf{Irr}(P)$ with respect to $\Rightarrow_R$ is equal to

$$\begin{aligned} \{i_P(x_1) \cdots i_P(x_n) : \forall i,\ 1 \leq i \leq n,\ x_i \in P \setminus \{1_P\}\ , \\ \forall i,\ 1 \leq i < n,\ (x_i, x_{i+1}) \notin \mathsf{dom}(\times)\}\ . \end{aligned} \tag{2}$$

In particular it contains the empty word ϵ obtained for $n = 0$, and every element of $P \setminus \{1_P\}$ (under the form $i_P(x)$). In case P is a (total) monoid, then $\mathsf{Irr}(P) = i_P(P \setminus \{1_P\}) \cup \{\epsilon\}$.

Note 2. Since each $u \in \mathsf{Irr}(P) \setminus \{\epsilon\}$ belongs to P^*, then u has a unique decomposition of the form $i_P(x_1) \cdots i_P(x_n)$, $x_i \in P \setminus \{1_P\}$, $1 \leq i \leq n$, $(x_i, x_{i+1}) \notin \mathsf{dom}(\times)$, $1 \leq i < n$.

Note that $\mathsf{Irr}(P)$ is prefix-closed[1]. Recall that u is a prefix of v if, and only if, there is $u' \in P^*$ such that $v = uu'$. Let $u \leq_P v$ be the relation " u is a prefix of v ". This partial order relation on P^* satisfies $u \leq_P v$ and $u' \leq_P v$ implies that u and u' are comparable, *i.e.*, $u \leq_P u'$ or $u' \leq_P u$ (see [6]). In what follows, $\mathsf{Pref}(w)$ denotes the set $\{u \in P^* : u \leq_P w\}$ of all prefixes of w, totally ordered by the restriction of $\leq_P$.

4.2 Discussion about the confluence

Let P be a partial monoid and R be its associated semi-Thue system. In general, R is not confluent (since it is not locally confluent). Indeed, the critical pair $(i_P(ab)i_P(a), i_P(a)i_P(ba))$ obtained from example 1.2 is not convergent. We call *essential* any critical pair of the form $((i_P(a)i_P(z), i_P(x)i_P(b))$ such that there is some $y \in P$ with $(x, y) \in \mathsf{dom}(\times)$, $(y, z) \in \mathsf{dom}(\times)$, $x \times y = a$ and $y \times z = b$.

Lemma 2. *The semi-Thue system R is confluent if, and only if, every essential critical pair converges.*

An essential critical pair may be trivial (take $y = 1_P$) so we try now to figure out those on which local confluence relies. The set of all essential critical pairs may be decomposed into several subsets. Let $(u, v) = (i_P(a)i_P(z), i_P(x)i_P(b))$ be an essential critical pair which comes from an overlap ambiguity $i_P(x)i_P(y)i_P(z)$ with $(x, y) \in \mathsf{dom}(\times)$, $x \times y = a$ and $(y, z) \in \mathsf{dom}(\times)$, $y \times z = b$. We say that (u, v) is of *type (A)* if $(a, z) \notin \mathsf{dom}(\times)$ (and therefore $(x, b) \notin \mathsf{dom}(\times)$). The critical pair (u, v) is of *type (B)* if $(a, z) \in \mathsf{dom}(\times)$ (and therefore $(x, b) \in \mathsf{dom}(\times)$): such a critical pair is convergent. The two types are obviously disjoint and cover all the essential critical pairs. We also say that a critical pair $(u, v) = (i_P(a)i_P(z), i_P(x)i_P(b))$ of type (A) (so $(a, z) \notin \mathsf{dom}(\times)$, $(x, b) \notin \mathsf{dom}(\times)$) is of *type (A1)* if $a = x$, $b = z$ (so in particular $(x, z) \notin \mathsf{dom}(\times)$); we immediately notice that a critical pair of type (A1) is trivial. A pair of type (A) is said to be of *type (A0)* if $u = i_P(a)i_P(z)$, $v = i_P(x)i_P(b)$, and $a \neq x$ or $b \neq z$. Types (A0) and (A1) are disjoint (in the second case $u = v$ while in the first one $u \neq v$). Each essential critical pair of type (A) is either of type (A0) or of type (A1).

Lemma 3. *The semi-Thue system R is confluent if, and only if, there is no critical pair of type (A0), or equivalently, if, and only if, each essential critical pair of type (A) is of type (A1).*

[1] It is also closed under factors [6].

Proof. The above discussion shows that the only possible non convergent essential critical pairs are of type (A0). Suppose that $(u, v) = (i_P(a)i_P(z), i_P(x)i_P(b))$ is an essential critical pair of type (A0), *i.e.*, $(a, z) \notin \mathsf{dom}(\times)$, $(x, b) \notin \mathsf{dom}(\times)$, $x \neq a$ or $z \neq b$, and there is $y \in P$ with $(x, y) \in \mathsf{dom}(\times)$, $x \times y = a$, $(y, z) \in \mathsf{dom}(\times)$, $y \times z = b$, $(\ell_1, r_1) = (i_P(y)i_P(z), i_P(y \times z))$, $(\ell_2, r_2) = (i_P(x)i_P(y), i_P(x \times y))$. From the assumptions we deduce that $x \neq 1_P$ (otherwise $(y, z) \notin \mathsf{dom}(\times)$), $z \neq 1_P$ (otherwise $(x, y) \notin \mathsf{dom}(\times)$) and $y \neq 1_P$ (otherwise $x = a$ and $z = b$). Moreover $a = x \times y \neq 1_P$ (otherwise $(1_P, z) = (x \times y, z) \notin \mathsf{dom}(\times)$), $b = y \times z \neq 1_P$ (otherwise $(x, 1_P) = (x, y \times z) \notin \mathsf{dom}(\times)$). So no rewriting rule can be applied on u or on v. Since $u \neq v$ (by assumption), (u, v) is not convergent. Suppose that R is confluent. So by lemma 2, every essential critical pair is convergent. But critical pairs of type (A0) cannot be convergent, so in this case, there is no such critical pair. □

Example 2. Let $P = \{1, x, y, z\}$ be a set with four elements equipped with a product $\times$ for which the only non trivial pairs (*i.e.* pairs without occurrences of the identity 1) in its domain are $(x, y), (y, y)$ and (y, z). We suppose that $x \times y = x$, $y \times y = y$ and $y \times z = z$. Then R is confluent because there is no critical pair of type (A0).

Confluence is obtained for a rather important class of partial monoids. A partial monoid P is called *catenary associative* (see [22] for the definition of " catenary associativity " in a partial magma, which is adapted for our purpose; see also [14]) if, and only if, for all $x, y, z \in P$, if $y \neq 1_P$, $(x, y) \in \mathsf{dom}(\times)$ and $(y, z) \in \mathsf{dom}(\times)$, then $(x \times y, z) \in \mathsf{dom}(\times)$ (and also $(x, y \times z) \in \mathsf{dom}(\times)$ by associativity in any partial monoid). We need that $y \neq 1_P$ otherwise the monoid would be total. None of the monoids of example 1 is catenary associative. Every (total) monoid is catenary associative. The set of arrows of a small category (see [23]) together with an adjoined total identity (and the obvious extension of composition) is a catenary associative partial monoid. It is easy to prove that in the catenary case there is no critical pair of type (A0).

Lemma 4. *Let P be a partial monoid. If P is catenary associative, then the semi-Thue system R is confluent.*

Partial monoids from example 1 have non confluent associated semi-Thue systems while the monoid of example 2 is not catenary but R is confluent.

4.3 Left standard reduction

In order to get a unique normal form property, even for non confluent semi-Thue system R, we restrict R by allowing only rewriting steps from " left to right ". This algorithm of reduction (informally described below) will ensure both termination and confluence, and therefore computes a unique normal form which is also a normal form for R.

1. `Input:` a word $w \in P^*$.
2. `Erase` all occurrences of $i_P(1_P)$ `in` w. `Result` $w' \in (P \setminus \{1_P\})^*$.

3. `While` $w' \notin \mathsf{Irr}(P)$ `do` let $r := i_P(x)i_P(y)$ be the first factor of w' (from left to right) such that $(x, y) \in \mathsf{dom}(\times)$. `If` $x \times y = 1_P$, `then erase` r from w' `else substitute` r by $i_P(x \times y)$ in w'.
4. `Output:` $w' \in \mathsf{Irr}(P)$.

First of all let $R_1 = \{(i_P(1_P), \epsilon)\}$. This semi-Thue system R_1 is terminating and confluent (since it has no critical pair). Thus every element of P^* has a unique normal form in $\mathsf{Irr}(R_1) = (P \setminus \{1_P\})^*$.

Lemma 5. *Let $w \in (P \setminus \{1_P\})^*$. Then*

1. $\mathsf{IrrPref}(w) = \mathsf{Irr}(P) \cap \mathsf{Pref}(w)$ *admits a maximum w_m (for the total order $\leq_P$ restricted to $\mathsf{IrrPref}(w)$);*
2. *$w_m = w$ if, and only if, $w \in \mathsf{Irr}(P)$;*
3. *If $w \notin \mathsf{Irr}(P)$, then there is a unique 4-tuple $(u, x, y, v) \in (P \setminus \{1_P\})^* \times (P \setminus \{1_P\}) \times (P \setminus \{1_P\}) \times (P \setminus \{1_P\})^*$ such that*
   (a) $w_m = ui_P(x)$;
   (b) $w = ui_P(x)i_P(y)v$;
   (c) $(x, y) \in \mathsf{dom}(\times)$.

Proof. First of all, $\mathsf{IrrPref}(w)$ is nonvoid because $\epsilon \in \mathsf{IrrPref}(w)$. Since $\mathsf{IrrPref}(w)$ is a subset of $\mathsf{Pref}(w)$ and as such is totally ordered by the restriction of $\leq_P$, it is sufficient to show that $\mathsf{IrrPref}(w)$ admits a maximal element, that is, an element $w_m \in \mathsf{IrrPref}(w)$ such that there is no $w' \in \mathsf{IrrPref}(w)$ with $w \leq_P w'$ and $w' \neq w$.

- Suppose that $w \notin \mathsf{Irr}(P)$. Since $w \in \mathsf{Irr}(R_1)$, that means that $|w| > 1$ and there is at least one integer i, $1 \leq i < |w|$ such that $w_i = i_P(x)$, $w_{i+1} = i_P(y)$, $(x, y) \in \mathsf{dom}(\times)$ and $x \neq 1_P$, $y \neq 1_P$. Let i_0 be the least such integer. Let $w_m = w_1 \cdots w_{i_0}$. Then, by definition of i_0, $w_m \in \mathsf{IrrPref}(w)$. Let $w' \in \mathsf{IrrPref}(w)$ such that $w_m \leq_P w'$. Then either $w_m = w'$ or $w'_{i_0} w'_{i_0+1}$ may be rewritten but in the latter case, $w' \notin \mathsf{Irr}(P)$.
- Suppose that $w \in \mathsf{Irr}(P)$. In this case, $w_m = w$. So we are done with (1). Note that the converse is obvious, and (2) holds.
- Concerning (3), let $w_{i_0} = i_P(x)$, $w_{i_0+1} = i_P(y)$ (with $x \neq 1_P$, $y \neq 1_P$ and $(x, y) \in \mathsf{dom}(\times)$). Let $u = w_1 \cdots w_{i_0-1}$ (thus $u = \epsilon$ if, and only if, $i_0 = 1$). Then $w_m = ui_P(x)$. Moreover $w = w_m w_{i_0+1} \cdots w_{|w|} = ui_P(x)i_P(y)v$ where $v = w_{i_0+2} \cdots w_{|w|}$ (thus $v = \epsilon$ if, and only if, $i_0 + 1 = |w|$). □

For $w \in (P \setminus \{1_P\})^* \setminus \mathsf{Irr}(P)$, the 4-tuple (u, x, y, v) of lemma 5 is called the *left-standard decomposition of* w, and denoted by $\mathsf{lstdecomp}(w)$.

Lemma 6. *Let $x \in P$ be a right (resp. left) invertible element. Then for every $y \in P$, $(y, x) \in \mathsf{dom}(\times)$ (resp. $(y, x) \in \mathsf{dom}(\times)$). In particular, if x is invertible, then every pair (x, y) and (y, x) belong to $\mathsf{dom}(\times)$*

Proof. Suppose that $x \in P$ is right (resp. left) invertible. Let $x' \in P$ such that $(x, x') \in \mathsf{dom}(\times)$ and $x \times x' = 1_P$ (resp. $(x', x) \in \mathsf{dom}(\times)$ and $x' \times x = 1_P$). Let $y \in P$ such that $(y, x) \notin \mathsf{dom}(\times)$ (resp. $(x, y) \notin \mathsf{dom}(\times)$). But $(y, x \times x') = (y, 1_P) \in \mathsf{dom}(\times)$ (resp. $(x' \times x, y) = (1_P, y) \in \mathsf{dom}(\times)$) and therefore, by associativity in P, $(y, x) \in \mathsf{dom}(\times)$ (resp. $(x, y) \in \mathsf{dom}(\times)$), that is, a contradiction. The last assertion of the lemma is straightforward. □

Lemma 7. *Let $u \in \mathsf{Irr}(P) \setminus \{\epsilon\}$ such that there is some $i \in \mathbb{N}$, $1 \leq i \leq |u|$ with $u_i = i_P(x)$ and x is right-invertible (resp. left-invertible). Then $i = 1$ (resp. $i = |u|$). In particular, if x is invertible, then $u = i_P(x)$.*

Proof. Suppose that $u_i = i_P(x)$ such that x is right (resp. left) invertible. According to lemma 6, for every $y \in P$, $(y, x) \in \mathsf{dom}(\times)$ (resp. $(x, y) \in \mathsf{dom}(\times)$). Now suppose that $i \neq 1$ (resp. $i \neq |u|$). Let $u_{i-1} = i_P(y)$ (resp. $u_{i+1} = i_P(y)$). Because u is irreducible, we have the contradiction $(y, x) \notin \mathsf{dom}(\times)$ (resp. $(x, y) \notin \mathsf{dom}(\times)$). The last assertion is trivial. □

Lemma 8. *Let $w \in (P \setminus \{1_P\})^* \setminus \mathsf{Irr}(P)$. Let $\mathsf{lstdecomp}(w) = (u, x, y, v)$. If $x \times y = 1_P$, then $u = \epsilon$, and, in particular, $w_m = i_P(x)$ (and therefore $\mathsf{IrrPref}(w) = \{\epsilon, i_P(x)\}$) and $\mathsf{lstdecomp}(w)$ has the form (ϵ, x, y, v).*

Proof. Suppose that $x \times y = 1_P$. Then, according to lemma 6, for every $z \in P$, $(z, x) \in \mathsf{dom}(\times)$ and $(y, z) \in \mathsf{dom}(\times)$. Now we can deduce that, since $ui_P(x) = w_m \in \mathsf{Irr}(P)$, then $u = \epsilon$ according to lemma 7. □

Lemma 9. *Let $A = \{w \in (P \setminus \{1_P\})^* \setminus \mathsf{Irr}(P) : \mathsf{lstdecomp}(w) = (\epsilon, x, y, v),\ x \times y = 1_P\}$ and $B = \{w \in (P \setminus \{1_P\})^* \setminus \mathsf{Irr}(P) : \mathsf{lstdecomp}(w) = (u, x, y, v),\ x \times y \neq 1_P\}$. Then $A \cap B = \emptyset$ and $A \cup B = (P \setminus \{1_P\})^* \setminus \mathsf{Irr}(P)$.*

Now let define $\rho_A = \{(w, v) \in A \times (P \setminus \{1_P\})^* : \mathsf{lstdecomp}(w) = (\epsilon, x, y, v)\}$ and $\rho_B = \{(w, w') \in B \times (P \setminus \{1_P\})^* : \mathsf{lstdecomp}(w) = (u, x, y, v),\ w' = ui_P(x \times y)v\}$. Both binary relations are functional (that is, $(x, y), (x, y') \in \rho_C$ implies that $y = y'$ for $C = A, B$). We write $\rho_C(w) = v$ for $(w, v) \in \rho_C$ ($C \in \{A, B\}$), in such a way that $\rho_A : A \to (P \setminus \{1_P\})^*$ and $\rho_B : B \to (P \setminus \{1_P\})^*$. It is not difficult to see that $\rho_A \cup \rho_B$ is a functional relation and a locally confluent abstract rewriting system on $(P \setminus \{1_P\})^*$ which is also terminating, and thus confluent. Moreover its set of normal forms is exactly $\mathsf{Irr}(P)$.

Let us consider the abstract rewriting system on P^*, called *left standard reduction*,

$$\mathsf{lstd}(R) = \Rightarrow_{R_1} \cup\ \rho_A \cup \rho_B\ . \tag{3}$$

The abstract rewriting system $\mathsf{lstd}(R)$ is terminating since the length of a word is reduced by any one-step reduction. We can also easily check that it is locally confluent, and therefore confluent. The set of irreducible elements with respect to $\mathsf{lstd}(R)$ is $\mathsf{Irr}(P)$.

Note 3. The many-step rewriting rule $\Rightarrow^*_{\mathsf{lstd}(R)}$ generated by $\mathsf{lstd}(R)$ and the equivalence relation $\Leftrightarrow^*_{\mathsf{lstd}(R)}$ generated by $\mathsf{lstd}(R)$ are respectively included in $\Rightarrow^*_R$ and $\Leftrightarrow^*_R$ (to prove this it is sufficient to see that $\mathsf{lstd}(R) \subseteq \Rightarrow^*_R$).

Since $\mathsf{lstd}(R)$ is terminating and confluent, for every $w \in P^*$, there is one and only one $w' \in \mathsf{Irr}(R)$ such that $(w, w') \in \mathsf{lstd}(R)^*$. Let $\mathsf{lstd} : P^* \to \mathsf{Irr}(P)$ be the mapping that maps a word to its normal form by $\mathsf{lstd}(R)$-reductions only.

Lemma 10. *Let $u, v, w \in P^*$ such that $(u, v) \in \mathsf{lstd}(R)$. Then $(uw, vw) \in \mathsf{lstd}(R)$.*

Proof. Suppose that there is at least one i such that $u_i = i_P(1_P)$, then only the reduction relation $\Rightarrow_{R_1}$ may be applied. In particular v is obtained by erasing (exactly) one occurrence of $i_P(1_P)$ from u, saying u_i. Therefore vw is obtained by erasing the same occurrence u_i in the prefix u of uw. Suppose that $w \in A \cup B$. If $w \in A$, then $\mathsf{lstdecomp}(u) = (\epsilon, x, y, v)$ and $v = \rho_A(u)$. Now $uw \in A$ and $\mathsf{lstdecomp}(uw) = (\epsilon, x, y, vw)$ in such a way that $\rho_A(uw) = vw$ as expected. Let suppose that $u \in B$. Let $\mathsf{lstdecomp}(w) = (u', x, y, v')$ (with $x \times y \neq 1_P$) in such a way that $v = u' i_P(x \times y) v'$. Then $uw \in B$ and $\mathsf{lstdecomp}(uw) = (u', x, y, v'w)$, so $\rho_B(uw) = u' i_P(x \times y) v' w = vw$. □

Lemma 11. *Let $u, v, w \in P^*$ such that $u \Rightarrow^*_{\mathsf{lstd}(R)} v$,* i.e.*, (u, v) belongs to the reflexive-transitive closure of $\mathsf{lstd}(R)$. Then $uw \Rightarrow^*_{\mathsf{lstd}(R)} vw$.*

Proof. Use the previous lemma several times. □

Lemma 12. *For every $u, v \in P^*$, $\mathsf{lstd}(\mathsf{lstd}(u)v) = \mathsf{lstd}(uv)$.*

Proof. By definition $u \Rightarrow^*_{\mathsf{lstd}(R)} \mathsf{lstd}(u)$. Therefore $uv \Rightarrow^*_{\mathsf{lstd}(R)} \mathsf{lstd}(u)v$ for any $v \in P^*$ according to the previous lemma. By uniqueness of the normal form, $\mathsf{lstd}(uv) = \mathsf{lstd}(\mathsf{lstd}(u)v)$. □

Note 4.
1. According to lemma 12, $\mathsf{Irr}(P)$ is a right P-module (see [11]).
2. In general the symmetric-reflexive-transitive closure $\Leftrightarrow^*_{\mathsf{lstd}(R)}$ of the left standard strategy $\mathsf{lstd}(R)$ is only a right congruence of P^*.
3. Let R, S be two binary relations on some set X. We say that R and S are *equivalent*, in symbol $R \equiv S$, if, and only if, $\Leftrightarrow^*_R = \Leftrightarrow^*_S$ (where $\Leftrightarrow^*_B$ is the equivalence relation generated by a binary relation B). Now suppose that R is itself confluent, then $\mathsf{lstd}(R) \equiv \Rightarrow_R$.

5 Monoid-like structures on $\mathsf{Irr}(P)$

No matter R be confluent or not, we can always equip $\mathsf{Irr}(P)$ with a monoid-like structure. However in general this operation is only associative up to the congruence $\Leftrightarrow^*_R$. For every $(u, v) \in \mathsf{Irr}(P)^2$, let us define $u \star v = \mathsf{lstd}(uv)$.

In general, $\star$ is not associative. For instance, let $x, y, z \in P$ such that $(x, y) \in \mathsf{dom}(\times)$, $x \times y = a$, $(y, z) \in \mathsf{dom}(\times)$, $y \times z = b$, and $(i_P(a)i_P(z), i_P(x)i_P(b))$ is a critical pair of type (A0). Then $(i_P(x) \star i_P(y)) \star i_P(z) = i_P(a)i_P(z)$, and $i_P(x) \star (i_P(y) \star i_P(z)) = i_P(x)i_P(b)$. Thus $(i_P(x) \star i_P(y)) \star i_P(z) \neq i_P(x) \star (i_P(y) \star i_P(z))$.

Lemma 13. *The operation $\star$ is " associative modulo $\Leftrightarrow^*_R$ ",* i.e.*, for all $u, v, w \in \mathsf{Irr}(P)$, $(u \star v) \star w \Leftrightarrow^*_R u \star (v \star w)$.*

Proof. On one side,

$$\begin{aligned}(u \star v) \star w &= \mathsf{lstd}(\mathsf{lstd}(uv)w) \\ &= \mathsf{lstd}((uv)w) \text{ (according to lemma 12)} \\ &= \mathsf{lstd}(u(vw)) \ ,\end{aligned} \tag{4}$$

on the other side, $u \star (v \star w) = \mathsf{lstd}(u\mathsf{lstd}(vw))$. According to note 3, $vw \Leftrightarrow_R^* \mathsf{lstd}(vw)$ (since for any $x \in P^*$, $x \Rightarrow_{\mathsf{lstd}(R)}^* \mathsf{lstd}(x)$, which implies that $x \Rightarrow_R^* \mathsf{lstd}(x)$, and therefore $x \Leftrightarrow_R^* \mathsf{lstd}(x)$). Because $\Leftrightarrow_R^*$ is a congruence of P^*, $u(vw) \Leftrightarrow_R^* u\mathsf{lstd}(vw)$. We conclude with the following sequence of equivalences.

$$\begin{aligned}(u \star v) \star v = \;& \mathsf{lstd}(u(vw)) \\ \Leftrightarrow_R^* \;& u(vw) \\ \Leftrightarrow_R^* \;& u\mathsf{lstd}(vw) \\ \Leftrightarrow_R^* \;& \mathsf{lstd}(u\mathsf{lstd}(vw)) \\ = \;& u \star (v \star w)\ .\end{aligned} \tag{5}$$

□

Actually it is possible to prove that bracketings are irrelevant for $\star$ in the sense that any other choice of bracketings for the product $(\cdots((x_1 \star x_2) \star x_3) \star \cdots) \star x_n)$ will evaluate to a normal form which is equivalent modulo the Thue congruence $\Leftrightarrow_R^*$. Let X be a set and $\mathsf{Mag}(X)$ be the free magma generated by X [8]. This set is equipotent to the free Σ-algebra generated by X with a unique symbol of function of arity 2 [13]: the set of all binary trees with leaves in X. Every element of $\mathsf{Mag}(X) \setminus X$ may be written in a unique way as $t_1 t_2$ ($t_1, t_2 \in \mathsf{Mag}(X)$). Let $\mathsf{Ass} = \{((t_1 t_2)t_3, t_1(t_2 t_3)) : t_1, t_2, t_3 \in \mathsf{Mag}(X)\}$. We extend this binary relation to a term rewriting system $\Rightarrow_{\mathsf{Ass}}$ on $\mathsf{Mag}(X)$ in the usual way (see [1]) which allows us to rewrite a subtree of the form $(t_1 t_2)t_3$ in a given tree. This term rewriting system is terminating. To see that, it is sufficient to check that the *rank*[2] $\mathsf{rk} : \mathsf{Mag}(X) \to \mathbb{N}$ of a tree, defined by $\mathsf{rk}(x) = 0$ for every $x \in X$ and $\mathsf{rk}(t_1 t_2) = \mathsf{rk}(t_1) + \mathsf{rk}(t_2) + \ell(t_1) - 1$ where $\ell(t)$ is the number of leafs of t ($\ell(x) = 1$ for every $x \in X$), strictly decreases at each application of a rewriting rule. Note that $\mathsf{rk}(t) = 0$ if all closing brackets are in backside position. Moreover Ass is locally confluent: the only critical pairs (see [1] for a general notion of critical pairs for term rewriting systems, see also [12]) comes from an overlap of $((xy)z)w$ (this is basically due to the consideration of the most general unifier between the subterm xy of the term $(xy)z$ and $(xy)z$ itself). So the critical pair is $((x(yz))w, (xy)(zw))$ given by two different applications of $\Rightarrow_{\mathsf{Ass}}$ on the tree $((xy)z)w$. This critical pair converges (it satisfies Stasheff's pentagon [27], made famous in [23]). Since $\Rightarrow_{\mathsf{Ass}}$ is terminating, it is confluent, which is not amazing at all since the rule $(xy)z \to x(yz)$ provides a " canonical system " for the variety of semigroups [21]. As usually $\Rightarrow_{\mathsf{Ass}}^*$ denotes the reflexive-transitive closure of $\Rightarrow_{\mathsf{Ass}}$. Now, $(\mathsf{Irr}(P), \star)$ is also a magma. Let $\mathsf{ev} : \mathsf{Mag}(\mathsf{Irr}(P)) \to \mathsf{Irr}(P)$ be the unique homomorphic extension of the identity, called the *morphism of evaluation* (see [20] for the definition of such a morphism in any Σ-algebra). For every $x \in \mathsf{Irr}(P)$, $\mathsf{ev}(x) = x$ and $\mathsf{ev}(t_1 t_2) = \mathsf{ev}(t_1) \star \mathsf{ev}(t_2)$.

Proposition 1. *Let $t_1, t_2 \in \mathsf{Mag}(\mathsf{Irr}(P))$. If $t_1 \Rightarrow_{\mathsf{Ass}}^* t_2$, then $\mathsf{ev}(t_1) \Leftrightarrow_R^* \mathsf{ev}(t_2)$.*

Proof. According to lemma 13, if $(t_1, t_2) \in \mathsf{Ass}$, then $\mathsf{ev}(t_1) \Leftrightarrow_R^* \mathsf{ev}(t_2)$. By structural induction on $\mathsf{Mag}(\mathsf{Irr}(P))$ we easily prove that if $t_1 \Rightarrow_{\mathsf{Ass}} t_2$, then

[2] Inspired from the rank of [23] used for the coherence theorem of monoidal categories.

$\mathsf{ev}(t_1) \Leftrightarrow_R^* \mathsf{ev}(t_2)$. Finally, by transitivity of $\Leftrightarrow_R^*$, from $t_1 \Rightarrow_{Ass}^* t_2$, we deduce that $\mathsf{ev}(t_1) \Leftrightarrow_R^* \mathsf{ev}(t_2)$ as expected. □

Roughly speaking this result means that the order of the evaluation of $\star$ products is irrelevant with respect to the Thue congruence. We cannot expect more from a non confluent semi-Thue system R (see proposition 2).

Note 5. A similar result may be obtained in a more general context: let $(M, *)$ be a magma and $\cong$ a congruence [8] on M. Suppose that for every $x, y, z \in M$, $(x * y) * z \cong x * (y * z)$. The following statement holds: for every $t, t' \in \mathsf{Mag}(M)$, if $t \Rightarrow_{\mathsf{Ass}}^* t'$, then $\mathsf{ev}(t) \cong \mathsf{ev}(t')$ (where $\mathsf{ev} : \mathsf{Mag}(M) \to M$ is the corresponding evaluation morphism).

Proposition 2. *The operation $\star$ is associative if, and only if, R is confluent.*

Proof. Suppose that R is confluent. According to remark 4, $\mathsf{lstd}(R) \equiv \Rightarrow_R$, *i.e.*, $\Leftrightarrow_{\mathsf{lstd}(R)}^* = \Leftrightarrow_R^*$. Therefore we can replace each occurrence of $\Leftrightarrow_R^*$ by an occurrence of $\Leftrightarrow_{\mathsf{lstd}(R)}^*$ in the sequence of equivalences (5) of the proof of lemma 13. We obtain $(u \star v) \star w = \mathsf{lstd}(uvw) \Leftrightarrow_{\mathsf{lstd}(R)}^* \mathsf{lstd}(u\mathsf{lstd}(vw)) = u \star (v \star w)$. Since there is one and only normal form in each equivalence class modulo $\Leftrightarrow_R^*$, we have $\mathsf{lstd}(uvw) = \mathsf{lstd}(u\mathsf{lstd}(vw))$, and thus $(u \star v) \star w = u \star (v \star w)$. Conversely, suppose that $\star$ is associative. Let $(i_P(a)i_P(z), i_P(x)i_P(b))$ be a critical pair of type (A0), that is, there is some $y \in P$ such that $(x, y) \in \mathsf{dom}(\times)$, $x \times y = a$, $(y, z) \in \mathsf{dom}(\times)$, $y \times z = b$, $(a, z) \notin \mathsf{dom}(\times)$ and $x \neq a$ or $z \neq b$. Then $(i_P(x) \star i_P(y)) \star i_P(z) = i_P(a)i_P(z) \neq i_P(x)i_P(b) = i_P(x) \star (i_P(y) \star i_P(z))$, which contradicts the assumption. Therefore there is no critical pair of type(A0), and by lemma 3, R is confluent. □

Note 6. Clearly, if R is confluent, then $\mathsf{Irr}(P)$ is isomorphic to $P^*/\Leftrightarrow_R^*$. Moreover, if P is a usual monoid, then $\phi : \mathsf{Irr}(P) = i_P(P \setminus \{1_P\}) \to P$ defined by $\phi(\epsilon) = 1_P$, and $\phi(i_P(x)) = x$ is an isomorphism of monoids.

References

1. Baader, F., Nipkow, T.: *Term rewriting and all that*. Cambridge University Press, 1999
2. Baer, R.: Free Sums of Groups and Their Generalizations. An Analysis of the Associative Law. American Journal of Mathematics. **71**(3) (1949) 706–742
3. Bessis, D.: The dual braid monoid. Ann. Scient. Éc. Norm. Sup. 4^e série, t. 36 (2003) 647–683
4. Bessis, D., Digne, F., Michel J.: Springer theory in braid groups and the BirmanKoLee monoid. Pacific J. Math. **205** (2002) 287-310
5. Bergman, G.M.: The diamond lemma for ring theory. Advances in Mathematics. **29** (1978) 178–218
6. Berstel, J., Perrin, D., Reutenauer, C.: *Codes and Automata*, volume 129 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2009
7. Book, R.V., Otto, F.: *String-rewriting systems*, *Texts and Monographs in Computer Science*. Springer-Verlag, 1993

8. Bourbaki, N.: *Algebra - chapters 1-3*. Springer, 1989
9. Bruck, R.H.: *A survey of binary systems*, Springer-Verlag, 1958
10. Duchamp, G.H.E., Poinsot, L., Goodenough, S. and Penson, K.A.: Statistics on Graphs, Exponential Formula and Combinatorial Physics. In Proceedings of the *3rd International Conference on Complex Systems and Applications - ICCSA 2009*, Le Havre, France, (2009) 60-63
11. Eilenberg, S.: *Automata, languages, and machines, vol. 1*, volume 59 of *Pure and applied mathematics*. Academic Press, 1976
12. Germain, C., Pallo, J.: Langages rationnels définis avec une concaténation non-associative. Theoretical Computer Science. **233** (2000) 217–231
13. Grätzer, G.: *Universal Algebra*. D. Van Nostrand Company, Inc., 1968
14. Gudder, S.P.: Partial algebraic structures associated with orthomodular posets. Pacific Journal of Mathematics. **41**(3) (1972) 717–730
15. Huet, G.: Confluent reductions: abstract properties and applications to term rewriting systems. Journal of the ACM. **27**(4) (1980) 797–821
16. Huet, G.: A Complete Proof of Correctness of the Knuth-Bendix Completion Algorithm. J. Computer and. System Sciences **23** (1981) 11–21
17. Jantzen, M.: *Confluent string rewriting*, volume 14 of *EATCS monographs on theoretical computer science*. Birkhäuser, 1988
18. Knuth, D.E., Bendix, P.B.: Simple word problems in universal algebras. In Computational Problems in Abstract Algebra (Ed. J. Leech), (1970) 263-297
19. Lafont, Y.: Algebra and geometry of rewriting. Applied Categorical Structures. **14**(4) (2007) 415–437
20. Lalement, R.: *Logique, réduction, résolution. Études et recherches en informatique*. Masson, 1990
21. Le Chenadec, P.: *Canonical forms in finitely presented algebras. Research Notes in Theoretical Computer Science*. Pitman, John Wiley & Sons, Inc., 1986
22. Ljapin, E.S., Evseev, A.E.: *The theory of partial algebraic operations*, volume 414 of *Mathematics and its applications*. Kluwer Academic, 1997
23. Mac Lane, S.: *Categories for the working mathematician (second ed.)*, volume 5 of *Graduate Texts in Mathematics*. Springer, 1997
24. Newman, M.H.A.: On theories with a combinatorial definition of 'equivalence'. Annals of Mathematics. **43** (1942) 223–243
25. Segal, G.: Configuration-spaces and iterated loop-spaces. Invent. Math. **21**(3) (1973) 213–221
26. Smith, P.A.: The complex of a group relative to a set of generators. Part I. Annals of Mathematics. **54**(2) (1951) 371–402
27. Stasheff, J.D.: Homotopy Associativity of H-Spaces. I. Transactions of the American Mathematical Society. **108**(2) (1963), 275–292
28. Tamari, D.: Le problème de l'associativité des monoïdes et le problème des mots pour les demi-groupes; algèbres partielles et chaînes élémentaires. Séminaire Dubreil-Pisot (Algèbre et Théorie des Nombres). **8** (1971) 1–15
29. Terese: *Term rewriting systems*, volume 55 of *Cambridge tracts in theoretical computer science*. Cambridge University Press, 2003
30. Wilce, A.: Partial Abelian semigroups. Intern. J. Theor. Phys. **34**(8) (1995) 1807–1812